

IT Security Standard:

Patch Management

Introduction

This standard defines specific procedural and configuration elements needed to implement the Bellevue College policy # 5250: Information Technology (IT) Security with regard to keeping computer systems and software current when software manufacturers issue updates to their systems and applications to improve software security. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all computing and computing-related technologies on campus. Compliance is expected of all campus users authorized to use or support those technologies. It is intended to specifically articulate a framework for formal software update management procedures which support all Bellevue College security expectations and industry best practices.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

Bellevue College relies on modern technology to support the business and educational operations of the college. The college has a complex technical infrastructure and a large number of individual networking components, including server and desktop hardware, upon which multiple software-based operating systems and applications are installed.

Each software application has technological weaknesses and vulnerabilities which may be exploited by people with malicious intent attempting to disrupt the educational and administrative missions of the college. As technology becomes more critical to day-to-day institutional functions the impact of the loss of those resources through vulnerability exploitation is increasing, as are the varieties of potential attacks.

Modern software manufacturers provide periodic security and/or functional updates—or “patches”—to existing applications or operating systems in order to better secure that software against the manipulation of vulnerabilities. In addition, these patches are disseminated in response to specific threats that have been identified. Failure by Bellevue College employees to apply these software updates in a timely manner increases the vulnerability of all Bellevue College technology and increases the likelihood that an attack will disrupt services.

Given the high level of dependence on the Bellevue College infrastructure and its software and hardware components, the most significant threats resulting from not keeping applications up-to-date are:

1. Malicious and/or unauthorized access to or modification of data
2. Vulnerability to malicious and/or accidental damage to resources
3. Malicious and/or accidental modification of networking components
4. Malicious and/or accidental denial/loss of service

In assessing the nature of the Bellevue College asset and the associated threats, the primary risk associated with failure to appropriately update technology on campus is to compromise services, resulting in loss of access to the technology—essentially a loss of service. This loss of service could have associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and a loss of reputation.

Secondary to this threat is the potential for inappropriate use of the resources, including: violations of state and/or federal law, uses inconsistent with Bellevue College's mission, and uses in violation of Bellevue College policy.

Standard

A. Responsibilities

1. The appropriate management of the Bellevue College infrastructure is truly a collaborative effort, involving Information Resources, its personnel and sub-units, and all campus users as a whole. With regard to the management of updates, these responsibilities include:
2. **Information Resources IT Management Team (ITMT)**
 - a. The Information Resources IT Management Team is comprised of the Dean of Information Resources and the technical support supervisors and administrators assigned to IR. The ITMT will:
 - i. Consult and assist as needed with regard to implementation of this standard.
 - ii. Approve all exceptions to this standard.
3. **Network Server Group (NSG)**
 - a. The Network Server Group is comprised of the systems and network administrators assigned primary responsibility within IR for the day-to-day management and maintenance of the Bellevue College networks and networked infrastructure. The NSG is a subsidiary unit within Computing Services (CS), which is itself a subsidiary unit of IR. The NSG will:
 - i. Adopt a formal, written patch management plan designed to carry out the expectations of this standard. This plan will:
 - a) be created under the direction of the Director of Computing Services, with consultation from ITMT and ITSA, as appropriate. This plan and any subsequent modifications should be approved through the ITMT.
 - b) identify those individual NSG members responsible for implementation and management of the plan.
 - c) articulate reasonable, minimal time frames for patch implementation for each type of hardware and software installed on campus.
 - d) require the use of automated update tools, if possible, to minimize windows of vulnerability
 - e) follow industry best practices. This should include processes that assess, test and implement patches regularly.

- f) include procedures for regular and routine application of patches if a software manufacturer releases software patches on a scheduled basis.
 - g) include provisions allowing scheduled network down-time for maintenance and updates, if required, and setting expectations for communication of those planned outages to the campus.
 - h) be reviewed and updated as necessary to remain current with technological advancements.
- b. With the proliferation of software vulnerabilities and modern developments such as “zero-day” attacks (a malicious attack developed almost simultaneously with the disclosure of vulnerability), it is mandatory that the college keep consistently apprised of software security issues and the status of software fixes for on-going issues.
- i. The NSG will monitor industry information sources on a daily basis to identify and respond appropriately to vulnerabilities.
 - a) In conjunction with this, the NSG will work with agencies such as the Washington Computer Incident Response Center (WACIRC), Microsoft, CERT, SANS and other vendors and organizations that offer alert services and support.
 - b) The NSG will consult with the ITMT—as appropriate—to monitor industry information sources and maintain up-to-date information regarding vulnerabilities.
- c. The NSG will have primary responsibility for:
- i. Identifying and testing software patches before they are distributed to campus computers.
 - ii. Carrying out the provisions of the patch management plan.

4. IT Support Personnel

- a. Defined as those individuals in Computing Services holding IT support classifications who are assigned desktop support and Help Desk responsibilities. The CS IT support personnel will:
- i. Assist the NSG in managing and updating software and software patches and fixes on the Bellevue College network.
 - ii. Ensure that these standards are met when installing, updating or troubleshooting Bellevue College systems.
 - iii. Be responsible for assisting general campus users in understanding and meeting the expectations of this standard.

5. IT Security Administrator (ITSA)

- a. The IT Security Administrator reports to the Dean of Information Resources and is assigned primary oversight of network and technology security. The ITSA is responsible for maintenance and implementation of the tenets of the Bellevue College IT Security Program and is a member of the ITMT. The ITSA:
- i. Will consult with and assist the NSG and CS IT support personnel in carrying out their responsibilities.
 - ii. Will document all exceptions to this standard.

6. General Campus Users

- a. This includes all users of Bellevue College computing and networking systems.
- i. Those college personnel with information regarding vulnerabilities that may affect Bellevue College systems will notify the NSG or the ITSA, who will investigate and respond appropriately.

- ii. If Bellevue College technology users are delegated responsibilities which include patch management, they are expected to meet all expectations articulated in this standard.

B. General Expectations

1. All security updates addressing specifically identified vulnerabilities in operating systems or applications will be applied as quickly and safely as is reasonably possible after a software manufacturer announces availability of a patch.
 - a. This includes all network, e-mail and web servers as well as desktop computers and other personal computing devices.
 - b. Patches may be distributed through the Bellevue College networks, if appropriate. This distribution may be an automatic process.
 - c. For systems or devices where automatic updates cannot be accomplished (such as remote computers or disconnected laptop/tablets):
 - i. Patches may be distributed via removable storage media to users holding appropriate security privileges for the user to install.
 - ii. Users may be directed to a software manufacturer's online update service with instructions to self-install the update.
 - iii. Pursuant to the Bellevue College IT security standard addressing "*Portable Computer System Usage*", updates and patches will be verified and/or applied to loaned equipment when presented to Computing Services for annual maintenance.
2. Only software patches and "fixes" that have been publicly-distributed by the specific software manufacturer responsible for the application or operating system will be applied.
 - a. If technically required, exceptions to this standard for appropriate, tested third-party patches may be granted, but must be specifically approved by the ITMT and documented by the ITSA as an exception.
3. IR will upgrade, replace or eliminate computers and servers connected to the Bellevue College network which are running versions of software no longer supported by the manufacturer. Exceptions will be handled as described in "*Unpatched Systems*", below.
4. The intent of this standard is that the risk to Bellevue College resources from malicious software or attacks be minimized as much as possible, with as little disruption to the business and academic functions of the college.
 - a. Any practice which supports this intent may be appropriate, including the specific procedures identified in this standard. However, because of the potential impact of exploited vulnerabilities, variations from the patch management plan and/or this standard must be approved through the ITMT.

C. Unpatched Systems

1. Recommended patches will be regularly installed on all servers and computers unless specific vendor applications prevent installation of current patches. Such cases will be documented as an exception to this standard.
2. If a specific business or educational function requires that a computer system remain unpatched, the following will apply:
 - a. The NSG and ITMT will be notified of the vulnerable system.
 - b. If the system does not require network access, it will be removed from the network.
 - c. If it is not possible to remove the system from the network, it will be isolated within the network to protect the overall resources.

D. New/Reconfigured Systems

1. Extra caution will be taken when setting-up new or reconfigured devices because these systems are particularly vulnerable until patched. As described in the Bellevue College IT

security standards addressing “Windows Base System Configuration” and “Macintosh Base System Configuration,” these precautions include:

- a. All relevant patches will be applied to the device prior to connecting to the network, if possible. Off-line methods such as manually-produced CDs or other storage media will be used when possible.
- b. All cumulative, up-to-date security and recommended patch bundles will be applied.
- c. If necessary, systems may be carefully attached by IT support personnel to “production” networks for installation, but no system may be used on any Bellevue College network in a production capacity until fully patched and security-hardened.

E. Upgrades

1. Patching computer system or application software is applying an update to those systems and/or applications, but is not the same as “upgrading” them.
 - a. Full upgrades to new operating systems and application versions will be based on business or curriculum needs.
 - b. All decisions to upgrade operating systems or applications will be made by the Information Resources IT Management Team.
 - c. Decisions to upgrade campus systems will be made with in consultation with those campus users and groups affected by the upgrade.
 - d. Upgrades which affect all administrative systems of a specific class (i.e. Macintosh, Windows) require the approval of President’s staff.
 - e. Upgrades to Bellevue College operating systems or application software may only be performed by designated IT support personnel.

F. Additional Applicable Standards

1. NSG/ IT Support Personnel

- a. In addition to the requirements identified in this standard, the following standards address expectations regarding patch application. If applicable to their specific job assignments, all NSG members and IT support personnel are expected to be familiar with these requirements, as well as those identified below incumbent on general campus users:
 - i. Electronic Mail Configuration
 - ii. Internet Software Security
 - iii. MPE System Configuration
 - iv. Portable Computer System Usage
 - v. Portable Data Storage Devices
 - vi. Web Servers

2. Campus Users

- a. In some cases, general campus users may have responsibilities for maintaining Bellevue College systems away from campus or their personal systems attached to the Bellevue College network in an updated, patched state. In those situations, all expectations of this standard apply.
- b. In addition, the following standards address expectations for patch application in these circumstances:
 - i. Connecting Non-Bellevue College Equipment to the Bellevue College Network
 - ii. Remote Access to Bellevue College Systems
 - iii. Security Privileges

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A -- References

1. Bellevue College Policy #5250: *Information Technology (IT) Security*
2. Bellevue College IT Security Standard: *Connecting Non-Bellevue College Equipment to the Bellevue College Network*
3. Bellevue College IT Security Standard: *Electronic Mail Configuration*
4. Bellevue College IT Security Standard: *Internet Software Security*
5. Bellevue College IT Security Standard: *Macintosh Base System Configuration*
6. Bellevue College IT Security Standard: *MPE System Configuration*
7. Bellevue College IT Security Standard: *Portable Computer System Usage*
8. Bellevue College IT Security Standard: *Portable Data Storage Devices*
9. Bellevue College IT Security Standard: *Remote Access to Bellevue College Systems*
10. Bellevue College IT Security Standard: *Security Privileges*
11. Bellevue College IT Security Standard: *Web Servers*
12. Bellevue College IT Security Standard: *Windows Base System Configuration*

Effective Date:	May 1, 2007
Date Last Modified:	April 12, 2009